might invalidate established assumptions prompting the system to require a higher confidence level where the circumstances imply some unusual or suspicious behaviour. Such behaviour might reflect a change in routine or consumption patters and therefore reduce the reliability of assumptions about the transaction context. In such a case additional authentication may be required to carry out the 'unusual' transaction.

[0091] Embodiments such as these, may involve adaptive learning processes and application of statistical techniques to properly assess the security of the transaction context. However the scope of the invention is to be construed to include such variations and embodiments.

[0092] Thus the present invention provides an adaptive technique for authenticating a user in a transaction context. It is extensible to take into account large variations in both user behaviour and transaction context. The invention is also sufficiently flexible to be applied to a large variety of authentication contexts.

[0093] Although the invention has been described by way of example and with reference to particular embodiments it is to be understood that modification and/or improvements may be made without departing from the scope of the appended claims.

[0094] Where in the foregoing description reference has been made to integers or elements having known equivalents, then such equivalents are herein incorporated as if individually set forth.

1. A method of authenticating a users ability to carry out a transaction, the method including the steps of:

a user initiating an authentication request in order to carry out a secure transaction;

dynamically collecting and assessing a plurality of confidence parameters, said confidence parameters reflecting factors related to the security of the Transaction context; and

dynamically maintaining a confidence level based on the plurality of confidence parameters whereby if the confidence level drops below a predetermined confidence threshold, the transaction is not authenticated and if the confidence level exceeds a predetermined confidence threshold, the transaction is authenticated.

2. A method claimed in claim 1 wherein the predetermined confidence threshold reflects the sensitivity of the transaction.

3. A method as claimed in claim 1 or **2** wherein a static confidence window is defined in response to substantially static confidence parameters, the confidence window having an upper and lower limit reflecting an inherent upper and lower limit that the confidence level can reach.

4. A method as claimed in claim 3 wherein user authentication is inhibited if the confidence threshold of the transaction is outside the confidence window.

5. A method as claimed in any preceding claim wherein the user alters the confidence level, either autonomously or in response to an external request, by varying and/or adding one or more confidence parameters.

6 A method as claimed in any preceding claim wherein the confidence level varies with time and/or transaction context.

7. A method as claimed in any preceding claim, wherein the confidence level decays over time.

8. A method as claimed in any preceding claim wherein the confidence parameters include:

intrinsic context parameters such as user input device security, user location, user identity, multiple user co-location, time after users authentication request initiation, required transaction security level, required resource security level and the like; and/or

extrinsic context parameters such as changes in network characteristics, dynamic changes in the sensitivity of the transaction and the like.

9. A method as claimed in any preceding claim wherein the transaction corresponds to a user requesting access to a resource.

10. A method as claimed in any preceding claims wherein the confidence threshold changes as a function of the capability of the users input device.

11. A method as claimed in any preceding claim wherein the confidence level is determined based the confidence parameters and/or on accumulated statistical data relating to the behaviour of the user.

12. A system for dynamically authenticating a transaction including:

a confidence engine adapted to:

dynamically maintain at least one confidence level by monitoring a plurality of confidence parameters, the confidence level reflecting the security of the Transaction context;

ii. compare the derived confidence level with a predetermined confidence threshold, the confidence threshold reflecting the security required to perform the transaction:

iii. when the confidence level is below the confidence threshold, requesting new confidence parameters or varying existing confidence parameters; and

iv when the confidence level is above the confidence threshold, authenticating the transaction; and

v. a plurality of authentication means adapted to dynamically provide, to the confidence engine, confidence parameters relating to the security of the transaction context.

13. A system as claimed in claim 12 further including a rule database adapted to correlate the plurality of confidence parameters with the confidence level.

14. A system-as claimed in claim 12 or **13** further including a guard means adapted to act as a proxy for the resources which are the subject of the transaction.

15. A system as claimed in any one of claims 12 to 14 further including device means adapted so that the user can interact with the authentication system, wherein the device has an authentication level which is taken into account when authenticating the transaction.

* * * * *